TOM BARTON

UChicago & Internet2

NOVEMBER 18, 2015

MAGIC Update: InCommon and Global Federation Issues

Outline

- InCommon road map highlights
- Attribute release
- Federation Interoperability WG
- InCommon's eduGain time line
- Sirtfi - federated security incident response
- Baseline trust

- Roles I represent today in italics
  - 100% UChicago CISO
  - 25% Internet2
  - *InCommon Technical Advisory Committee member*
  - *REFEDS Steering Committee member*
  - Internet2 TIER Ad Hoc Advisory Chair

InCommon Road Map – Some Highlights

1. ***Attribute release***
2. ***IdP/SP practice requirements***
3. ***International interfederation***
4. Offer IdP for researchers without federated credentials
5. Understand our community
6. Operational security and operational continuity
7. User consent strategy
8. Streamline HE admissions process (CommIT)
9. ***Community practice trust framework***
10. Community MFA profile

→ ***16. Federated incident response***

Attribute Release

- Many things need attributes to work!
- Most important attributes: *email, name, persistent identifier*
- Frameworks for their release
  - R&S Entity Category
    - SPs that support research & scholarship
    - SP & IdP metadata tags (42 SPs & 118 IdPs currently in InCommon)
    - Global standard by REFEDS
  - Trusted federation
    - If they're in our public directory, every SP in our Federation can have them
  - User consent
- Barriers
  - Inability of Central IT to address policy questions, accept risks
  - Lack of communication between researchers and Central IT
  - Data Privacy for EU ↔ non-EU transactions
  - Lack of technology to "nudge" the right behavior

Federation Interoperability WG

- Improve IdP-SP interoperability by promoting interoperability of software implementations and deployment practices
- Participation: US & EU R&E, Ping, Microsoft, OCLC
- “SAML v2.0 Implementation Profile for Federation Interoperability”
  - Software conformance requirements for developers
  - Details the features that are necessary in order to use SAML metadata as a basis for secure, scalable, and extensible [*multilateral*] trust fabrics
  - Completion in December 2015
- Next steps:
  - REFEDS Consultation
  - Incorporation into Fed-Lab (http://fed-lab.org/)
  - Publication by Kantara
- Follow-on WG to address deployment practices
- Fed-Lab to be used by InCommon to verify product interop

InCommon's eduGain Time Line

Before	**423 IdPs & 2626 SPs in InCommon as of Nov 16, 2015**
Done	• Extend InCommon metadata procedures • Changes to "Federation Operating Policies & Practices" & "Participation Agreement" • Participants notified of changes and their options

Nov 20 2015	• Federation Manager UI enhancements:
	  • ***IdPs: opt-out from eduGain***
	  • ***SPs: opt-in to eduGain***

Jan 11 2016	• eduGain metadata included in InCommon's "preview" aggregate
Feb 11 2016	• eduGain metadata included in InCommon's production aggregate • InCommon entities exported to eduGain • Default Participation Agreement acceptance date
After	**More than 1800 IdPs & 3500 SPs**

Sirtfi & Federated Security Incident Response

- Overall goal: enable R&E Orgs to coordinate security incident response
- Sirtfi Phase 1 goal: establish global standard
- Sirtfi Trust Framework v1.0 defines low bar security incident response capabilities to which member organizations can self-assert compliance
  - Operational Security (patching, vulnerability management, intrusion detection, user access management)
  - Incident Response (contact info, willing to respond, Traffic Light Protocol)
  - Logging (available to aid Incident Response)
  - Policy (AUP exists)
- Under REFEDS Consultation now
- Submit to IETF as Independent RFC

Sirtfi Phase 2

Ability for one Org to contact others to initiate a response Scale: 10s of 1000s of R&E Orgs worldwide	
1. Get security contact info in R&E federation metadata	• CY2016 REFEDS WG to produce normative doc, recommended procedures, and promotional materials for use by R&E federation operators • Similar to R&S Entity Category specification
2. Establish Sirtfi v1.0 entity tag	
3. Demonstrate feasibility	• 2-3 R&E Federations • 2-3 members each • InCommon already has >200 entities with security contact info
4. Promote!	

Sirtfi Phase 3

- Goal: proactive notification by IdP to SP of account breach on need to know and private basis
- Blend three essential capabilities
  1. Tool used by IdP Org's security team to determine which SPs a compromised account has recently visited
  2. SP registration process to qualify need to know
  3. Infrastructure in which to combine 1 & 2 to signal SPs accordingly
- Potential Proof of Concept with Confyrm
  - Might cover 2 & 3
- R&E community develop tool #1 with AARC (EU) funding
- ID Events IETF BoF related work in OIDC realm
- Challenges: technical, policy, cultural

Baseline Trust

- What assurances do members of R&E Feds need of each other to be comfortable transacting with each other?
- FICAM/Kantara assurance profiles
  - Requires formal audit, too heavy
- InCommon's Participant Operating Practices
  - Hard to verify, too light
- New approach:
  - Five expectations of IDPs
  - Five expectations of SPs
  - Attestation communicated in a machine readable format
  - Create InCommon business and technical processes to hold IdPs and SPs accountable for attesting to baseline expectations
- Trustworthiness emerges from organizational maturity and commonality of practice. Internet2 TIER project should help orgs with those.

Potential Participant Baseline Expectations

Expectations of IdPs

1. The IdP is operated under the authority of the organization's InCommon executive contact
2. The IdP only presents assertions believed to be accurate
3. The IdP is trustworthy enough to access the organization’s enterprise systems
4. Federation metadata is accurate, complete, and includes site contacts, MDUI information, and privacy policy
5. Security incident response plan covers IdP operations

Expectations of SPs

1. Controls are in place to reasonably secure information and maintain user privacy
2. Information received from IdPs is stored only when absolutely necessary for SP’s purpose
3. Federation metadata is accurate, complete, and includes site contacts, MDUI information, and privacy policy
4. Documented attribute requirements are published
5. Security incident response plan covers SP operations

Baseline Trust – Next Steps

- Extreme baking of these formulations with InCommon community
- Establish as formal InCommon Participant requirement
- 1 year out??

- Of course, it is not enough that only one R&E federation have a trust baseline
- Some other R&E Feds address similar requirements by other means
- Possible future REFEDS activity to map them, identify gaps, establish common baseline trust standard and R&E Fed processes

QUESTIONS?

Tom Barton

tbarton@uchicago.edu